H.19 CAR 1352.239-73 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES (OCTOBER 2003) (Modified)

(a) This clause is applicable to all contracts that include information technology resources or services in which the Contractor must have physical or electronic access to USPTO's sensitive or classified information, which is contained in systems that directly support the mission of the Agency. For purposes of this clause, the term "Sensitive" is defined by the guidance set forth in:
(1) The DOC IT Security Program Policy and Minimum Implementation Standards http://www.osec.doc.gov/cio/ITSIT/DOC-IT-Security-Program-Policy.htm;
(2) The Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources (http://csrc.nist.gov/policies/appendix_iii.pdf), which states that there is a "presumption that all [general support systems] contain some sensitive information."; and
(3) The Computer Security Act of 1987 (P.L. 100-235) (http://www.epic.org/crypto/csa/csa.html), including the following definition of the term sensitive information "…any information the loss, misuse, or unauthorized access, to or modification of which could adversely affect the national interest or the, conduct of federal programs, or the privacy to which individuals are entitled under section 552 of title 5, United States Code (The Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

For purposes of this clause, the term "Classified" is defined by the guidance set forth in:
(1) The DOC IT Security Program Policy and Minimum Implementation Standards, Section 3.3.1.4 (http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf).
(2) The DOC Security Manual, Chapter 18 (http://www.easc.noaa.gov/Security/webfile/erso.doc.gov/5_2003%20Security%20Manual/DOC%20Manual%20of%20Security%20Policies%20and%20Procedures.htm).
(3) Executive Order 12958, as amended, Classified National Security Information. Classified or national security information is information that has been specifically authorized to be protected from unauthorized disclosure in the interest of national defense or foreign policy under an Executive Order or Act of Congress.

Information technology resources include, but are not limited to, hardware, application software, system software, and information (data). Information technology services include, but are not limited to, the management, operation (including input, processing, transmission, and output), maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. The Contractor shall be responsible for implementing sufficient Information Technology security, to reasonably prevent the compromise of USPTO IT resources for all of the contractor's systems that are interconnected with a USPTO network or USPTO systems that are operated by the Contractor.

(b) All Contractor personnel performing under this contract and Contractor equipment used to process or store USPTO data, or to connect to USPTO networks, must comply with the requirements contained in the USPTO IT Security Handbook.

(c) For all Contractor-owned systems for which performance of the contract requires interconnection with a USPTO network or that USPTO data be stored or processed on them, the Contractor shall:

(1) Provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The plan shall describe those parts of the contract to which this clause applies. The Contractor's IT Security Plan shall comply with federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq,) and the Federal Information Security Management Act of 2002, Pub. L. No. 107-347 Stat. 2899, 2946-2961 (2002); Pub. L. No. 107-296 Stat. 2135, 2259-2273 (2002). 38 WEEKLY COMP. PRES. DOC. 51,2174 (Dec. 23, 2002) (providing statement by President George W. Bush regarding Federal Information Security Management Act of 2002). The plan shall meet IT security requirements in accordance with Federal and USPTO policies and procedures that include, but are not limited to:

(a) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources (http://csrc.nist.gov/policies/appendix_iii.pdf);
(b) National Institute of Standards and Technology Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems (http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF); and
(c) DOC Procedures and Guidelines in the Information Technology Management Handbook (http://nsi.org/Library/Govt/docinfo.txt).
(d) National Industrial Security Program Operating Manual (NISPOM) for classified systems (http://www.dss.mil/isec/nispom.htm); and

(2) Upon award, the contractor shall register with the USPTO Certification and Accreditation Group (CACG), with copy to the Contracting Officer, to initiate the certification and accreditation process described in paragraph 3 below.

(3) Within 14 days after receipt of direction from the CACG, the contractor shall submit for USPTO approval a System Certification and Accreditation package, including the IT Security Plan and a system certification test plan, as outlined in USPTO Certification and Accreditation Technical Standard and Guideline. The Certification and Accreditation Package must be consistent with and provide further detail for the security approach contained in the offeror's proposal or sealed bid that resulting in the award of this contract and in compliance with the requirements stated in this clause. The Certification and Accreditation Package, as approved by the Contracting Officer, in consultation with the USPTO Security Officer, shall be incorporated as part of the contract. USPTO will

use the incorporated IT Security Plan as the basis for certification and accreditation of the contractor system that will process USPTO data or connect to USPTO networks. Failure to submit and receive approval of the Certification and Accreditation Package, as outlined above may result in termination of the contract.

(d) The Contractor shall incorporate this clause in all subcontracts that meet the conditions in paragraph (a) of this clause.